

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-100069

(P2000-100069A)

(43) 公開日 平成12年4月7日(2000.4.7)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 C 0 6 4
G 0 9 C 1/00	6 2 0	G 0 9 C 1/00	6 2 0 Z 5 D 0 4 4
	6 6 0		6 6 0 D 5 K 0 1 3
H 0 4 L 9/32		H 0 4 N 7/16	Z
H 0 4 N 7/16		H 0 4 L 9/00	6 7 5 Z

審査請求 未請求 請求項の数11 O L (全 15 頁)

(21) 出願番号 特願平10-267505

(22) 出願日 平成10年9月22日(1998.9.22)

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 石橋 泰博

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(72) 発明者 春木 耕祐

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(74) 代理人 100083161

弁理士 外川 英明

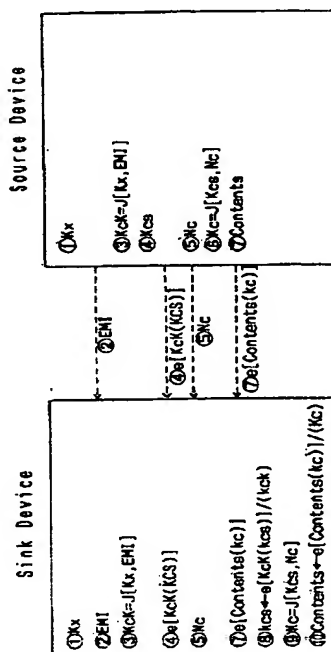
最終頁に続く

(54) 【発明の名称】 コピープロテクト方法、及び同方法を適用したデータ処理装置、並びに記録媒体

(57) 【要約】

【課題】各機器間で同一に暗号化されたコンテンツデータを共有し、かつ強固なコピープロテクト方法を実現する。

【解決手段】Source Deviceは、乱数発生器などにより発生されるシードキー(Kcs)を生成し、このシードキー(Kcs)を結合キー(Kck)を利用して暗号化を施し、暗号化されたシードキー(eKcs)をSink Deviceに送信する。またSource Deviceはコンテンツデータ(Contents)を暗号化、及び復号化するためのコンテンツキー(Kc)をシードキー(Kcs)と時変数データ(Nc)との関数に基づいて生成する。そして、Sink Deviceはコンテンツキー(Kc)を用いて、暗号化されたコンテンツデータ(e[Contents(KC)])を復号化する。



【特許請求の範囲】

【請求項 1】 暗号化鍵によって暗号化及び復号化可能なコピープロテクト対象のデータを授受するためのコピープロテクト方法において、

送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記暗号化鍵を生成するためのパラメータ情報を暗号化された状態で、前記送信元デバイスより受信すると共に、前記暗号化鍵により暗号化されたコピープロテクト対象のデータを受信し、

この受信したコピープロテクト対象のデータを、他の相手先デバイスに送信する場合、前記送信元デバイスより受信した前記パラメータ情報を暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送することを特徴とするコピープロテクト方法。

【請求項 2】 暗号化鍵によって暗号化及び復号化可能なコピープロテクト対象のデータを授受するためのコピープロテクト方法において、

送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記送信元デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される第 1 の認証情報を取得し、

前記送信元デバイスにより、前記第 1 の認証情報によって暗号化された前記暗号化鍵を生成するためのパラメータ情報を受信すると共に、暗号化されたコピープロテクト対象のデータを受信し、

受信した前記パラメータ情報の前記第 1 の認証情報による暗号化を解除し、

この受信したコピープロテクト対象のデータを、他の相手先デバイスに送信する場合、送信先となる相手先デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される第 2 の認証情報を取得し、

前記送信元デバイスより受信した前記暗号化鍵を生成するためのパラメータ情報を、前記第 2 の認証情報により暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送することを特徴とするコピープロテクト方法。

【請求項 3】 前記暗号化を解除するための情報は、所定の関数によって暗号化解除情報を生成することができるよう、複数のパラメータに分けられた情報であることを特徴とする請求項 2 記載のコピープロテクト方法。

【請求項 4】 前記複数のパラメータのうち少なくともひとつは前記第 1 または第 2 の認証情報によって暗号化され加えられ、送受信されることを特徴とする請求項 3 記載のコピープロテクト方法。

【請求項 5】 暗号化鍵により暗号化及び復号化可能なコピープロテクト対象のデータを扱うデータ処理装置にお

いて、

データを受信する受信手段と、

この受信手段に受信された情報を他のデバイスに送信する送信手段と、

前記他のデバイスとの間でコピープロテクト対象のデータを授受するための認証処理を行う認証手段とを具備し、

送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記認証手段により前記送信元デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される第 1 の認証情報を前記受信手段で取得し、

前記送信元デバイスにより、前記第 1 の認証情報によって暗号化された前記暗号化鍵を生成するためのパラメータ情報を前記受信手段で受信すると共に、暗号化されたコピープロテクト対象のデータを受信し、

前記認証手段により受信した前記パラメータ情報の前記第 1 の認証情報による暗号化を解除し、

この受信したコピープロテクト対象のデータを、他の相手先デバイスに送信する場合、前記認証手段で送信先となる相手先デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される第 2 の認証情報を前記受信手段で取得し、

前記送信手段により前記送信元デバイスより受信した前記暗号化鍵を生成するためのパラメータ情報を、前記第 2 の認証情報により暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送することを特徴とするデータ処理装置。

【請求項 6】 前記暗号化を解除するための情報は、複数のパラメータに分けられた情報であり、前記認証手段は、所定の関数によって前記複数のパラメータから暗号化解除情報を生成することを特徴とする請求項 5 記載のデータ処理装置。

【請求項 7】 前記複数のパラメータのうち少なくともひとつは、前記第 1 または第 2 の認証情報によって暗号化して送受信することを特徴とする請求項 6 記載のデータ処理装置。

【請求項 8】 前記暗号化鍵を生成するためのパラメータ情報をこのデータ処理装置固有の情報により暗号化して、格納する記録手段を具備したことを特徴とする請求項 5 記載のデータ処理装置。

【請求項 9】 暗号化されたコピープロテクト対象のデータを授受するためのコピープロテクト方法において、送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記送信元デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される認証情報を取得し、

この取得した前記認証情報を用いて結合情報を生成し、

前記結合情報を用いて暗号化した第1のパラメータ情報、及び時変数である第2のパラメータ情報を受け取り、
前記送信元デバイスより、第1及び第2のパラメータを用いて生成された暗号化情報により暗号化された前記コピープロテクト対象のデータを受け取り、
前記生成した結合情報によって前記第1のパラメータの暗号化を解除し、

この暗号化を解除された第1のパラメータ及び、第2のパラメータを用いて、前記コピープロテクト情報の暗号化を解除するための暗号化鍵を生成可能に保持すること
を特徴とするコピープロテクト方法。

【請求項10】 暗号化されたコピープロテクト対象のデータを授受するためのコピープロテクト方法において、

送信先デバイスへ前記コピープロテクト対象のデータを送信する場合、前記送信先デバイスとの間で認証処理を実施し、

この認証処理によって生成、共有される認証情報を取得し、

この認証情報を用いて暗号化した結合情報を前記送信先デバイスに送信し、

この結合情報を用いて暗号化された第1のパラメータ、及び時変数である第2のパラメータ情報を前記送信先デバイスに送信し、

前記第1のパラメータ及び第2のパラメータを用いて、暗号化のための暗号化情報暗号化鍵を生成し、

この暗号化情報に基づいて、前記コピープロテクト対象のデータを暗号化し、前記送信先デバイスに送信することを特徴とするコピープロテクト方法。

【請求項11】 コンピュータシステムによって読み出し可能な記録媒体であって、
コピープロテクト対象のデータが暗号化されて記録される第1の記憶領域と、

前記暗号化データの暗号化を解除する暗号化鍵を生成するために必要な情報を少なくとも第1及び第2の2つのパラメータに分けて記録する第2の領域を含み、前記第2の領域は、前記コンピュータシステムからは読み出せない領域であり、前記第1及び第2のパラメータは、コンピュータシステム内の複数のデバイスで共有可能な情報であることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンテンツデータを扱うパーソナルコンピュータにおけるコピープロテクト情報、及び同方法を適用したデータ処理装置、並びに記録媒体に関する。

【0002】

【従来の技術】近年、コンピュータ技術の発達に伴い、デジタルビデオプレーヤ、セットトップボックス、T

V、パーソナルコンピュータ等のマルチメディア対応の電子機器が種々開発されている。

【0003】この種の電子機器は、例えばDVD(Digital Versatile Disk)に蓄積された映画、デジタル衛星放送によるTV番組等のコンテンツデータを再生することができる。

【0004】コンテンツデータは一般にMPEG2という動画像高能率符号化方式を使って符号化された後、記録媒体や、伝送媒体を通じて各家庭に送られる。MPEG2による符号化は、画質と、容量に対する記録時間の双方を確保する観点から、可変レート符号化の考えに基づいている。可変レート符号化データのデータ量は、元の画像の画質に依存し、動きの激しいシーンほどそのデータ量は増加する。よって、コンテンツデータは、各家庭にオリジナル映像と遜色のない高画質の映像を提供することができる。

【0005】近年、このようなコンテンツデータの著作権保護等の観点から、その不正コピーを防止するためのコピープロテクト技術の必要性が叫ばれてきたが、有効な手法が構築されていないのが現状である。

【0006】そこで、CPTWG(Copy Protection Technical Working Group)では、マルチメディアデータの伝送に好適な次世代のバスインターフェイスであるIEEE1394シリアルバスに向けた新たなコピープロテクト方式の仕様(以下、IEEE1394コピープロテクト技術と称する)の策定作業が進められている。

【0007】IEEE1394シリアルバスは、デジタルビデオプレーヤ、セットトップボックス、TV、パーソナルコンピュータ等をつなぐ次世代のバスインターフェイスであり、転送モードとして、アシンクロナスサブアクションと、アイソクロナスサブアクションの2種類をサポートしている。前者は、非同期転送モードと呼ばれ、リアルタイム性が要求されない一般のデータの転送時に使用される。後者は、転送帯域を保証した同期転送モードであり、ビデオデータやオーディオデータに代表されるデジタルのコンテンツデータのリアルタイム転送が可能である。

【0008】IEEE1394コピープロテクト技術は、公開鍵暗号化方式や共通鍵暗号化方式などのよく知られた暗号化プロトコルを用いることにより、IEEE1394シリアルバスを介してデジタルビデオプレーヤ、セットトップボックス、TV、パーソナルコンピュータなどの各機能モジュール機器間(以下各機器間)で受け渡しされるコンテンツデータを暗号化し、その不正コピーを防止できるようにしている。

【0009】

【発明が解決しようとする課題】このように暗号化されたコンテンツデータを各機器間で受け渡しをした場合には、必然的にこの暗号化されたコンテンツデータの暗号

化を解除するための暗号化鍵(以下コンテンツキー)についても同機器間で受け渡しをする必要がある。しかし、このコンテンツキーが不正に取り出されてしまえば、コンテンツデータの暗号化を解除されてしまうことになるので、コンテンツキーをそのまま受信装置側に送信してしまうこと、或いは単にコンテンツキーを暗号化して送信するだけでは危険である。従って、このコンテンツキーについても不正コピーをされないように、各機器間で確実に受け渡しができるシステムを構築しなければならない。

【0010】そこで本願発明者は、コンテンツキー自体を受信装置側にそのまま送信することは避け、ある複数のパラメータを送って、予め決められた所定の関数により、受信装置側でコンテンツキーを作成する方式を模索検討した。以下、これについて具体的に説明する。

【0011】図8は、セットップボックス1(STB)からIEEE1394バス2を介して送信されてきたコンテンツデータをパーソナルコンピュータ3内の1394ブリッジ4を介してDVD-RAMドライブ5等のストレージデバイスに録画格納し、さらにMPEG2デ

コーダ6にコンテンツデータを渡し、ディスプレイ7で表示させる過程を想定している。

【0012】このシステムにおいて、まずSTB1からDVD-RAMドライブ5にコンテンツデータを送信する際、STB1とDVD-RAMドライブ5それぞれに設けられるAuthenticator8、9で機器間の認証処理が行われる。認証の方式は、各機器でそれぞれ保有している公開鍵暗号化方式等、よく知られた暗号化プロトコルを用いることにより、機器が正当なデバイスであることを確認しあう。そして、この認証処理の結果、お互いのデバイスでコントロールキーと呼ばれるパラメータ(Kx)が共有することができる。そしてさらに、CGMSと呼ばれるコピーコントロール情報(EMI)を送信する。(尚、このEMIの情報は、コピー回数を管理できる情報であり、コピー不可、コピー一回可、コピー可等の3種類情報を定義するものである。そして、コンテンツデータを他の機器にコピーする都度そのコピー可能な回数が削減され内容が書き換えられるものである。)この2つのパラメータを用いて、コンテンツキー(Kc)を受信側で作成する。従って例えばKcは下記のような関数で表現される。

【0013】 $Kc = J [Kx, f(EMI)]$

このようにすればコンテンツキー(Kc)自体を、送信側から受信側にそのまま送信する必要がなくなり、コピープロテクトをより確実に施すことができる。

【0014】そして、DVD-RAMドライブ5には、STB1のCipher10でコンテンツキー(Kc)を用いて暗号化されたコンテンツデータ(e[Contents(Kc)])とともに、コントロールキー(Kx)及びコピーコントロール情報(EMI)がパラメ

タとして格納されることになる。

【0015】次に、DVD-RAMドライブ5に格納されたコンテンツデータ(e[Contents(Kc)])を、MPEG2デコーダ6等の再生手段に正当に受け渡し、ディスプレイ7に表示させるまでの処理を説明する。

【0016】この時も、まずDVD-RAMドライブ5とMPEG2デコーダ6に設けられたAuthenticator9、61で認証処理が実施される。そして、上記STB1とDVD-RAMドライブ5との認証処理の時と同様に、コントロールキーを共有し、コピーコントロール情報をパラメータとして定め、この2種類のパラメータによる関数でコンテンツキーを作成する。

【0017】ただ、このときコントロールキー、コピーコントロール情報は、前回STB1とDVD-RAMドライブ5とで認証処理をした時とはデータが異なる。これは、コントロールキー(Kx)は各デバイス間同志で固有の認証処理によって生成される情報であるので各認証処理で異なるデータが生成されるためである。またEMIについては、例えば、コピー一回可データがSTB1からDVD-RAMドライブ5に格納された場合には、DVD-RAMドライブ5からMPEG2デコーダ6に送信される場合にはコピーコントロール情報が「これ以上コピー不可」を示す情報に書き換えられてから送信されてしまうからである。

【0018】つまり、上記とは異なり新たなコントロールキー(Kx')、と内容が変更されたコピーコントロール情報(EMI')のパラメータを用いるので、 $Kc' = J [Kx', Nc, f(EMI')]$ を作成することになる。

【0019】従って、DVD-RAMドライブ9は新たなコンテンツキー(Kc')を用いて、コンテンツデータを暗号化(e[Contents(Kc')])し、MPEG2デコーダ6に送信し、MPEG2デコーダ6では、2つのパラメータを用いて作成したコンテンツキーKc'を用いて、Cipherにてコンテンツデータを復号化して、ディスプレイに出力する。

【0020】以上がコンテンツキーをそのまま各機器に送信しないで、複数のパラメータの関数によりコンテンツキーを作成し、コンテンツデータを暗号化、復号化する方式の一例である。ただこの方式だと確実なコピープロテクト処理を施すことができるが、以下のような不具合が生ずる。

【0021】即ち、それぞれの機器に受け渡されるコンテンツデータは、同じ内容のデータであるにも関わらず、各機器間でそれぞれ異なるコンテンツキーを用いて、暗号化、復号化を実施しなければならないことである。言い換えれば、コンテンツキー(Kc)で暗号化されたコンテンツデータをコンテンツキー(Kc')で再度暗号化し直して、別の機器に受け渡すことしなければ

ならず、演算処理を多大な負荷をかけることになる。特にDVD-RAMドライブ等のストレージデバイスは演算能力が低いデバイスであり暗号化をすることは困難である。

【0022】本発明は上述の実情に鑑みてなされたものであり、暗号化されたコンテンツデータに対してさらに暗号化するような処理をすることなく、各機器間で同一に暗号化されたコンテンツデータを共有することができ、かつ強固なコピープロテクト機能を実現することが可能なデータ記録装置、同装置を用いたデータ処理システム及びコピープロテクト方法、並びに記録媒体を提供することを目的とする。

【0023】

【課題を解決するための手段】上述の課題を解決するため、本発明は、暗号化鍵によって暗号化及び復号化可能なコピープロテクト対象のデータを授受するためのコピープロテクト方法において、送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記暗号化鍵を生成するためのパラメータ情報を暗号化された状態で、前記送信元デバイスより受信すると共に、前記暗号化鍵により暗号化されたコピープロテクト対象のデータを受信し、この受信したコピープロテクト対象のデータを、他のデバイスに送信する場合前記送信元より受信した前記パラメータ情報を暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送するものである。

【0024】上述の課題を解決するため、本発明は、暗号化鍵によって暗号化及び復号化可能なコピープロテクト対象のデータを授受するためのコピープロテクト方法において、送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記送信元デバイスとの間で認証処理を実施し、この認証処理によって生成、共有される第1の認証情報を取得し、前記送信元デバイスにより、前記第1の認証情報によって暗号化された前記暗号化鍵を生成するためのパラメータ情報を受信すると共に、暗号化されたコピープロテクト対象のデータを受信し、受信した前記パラメータ情報の前記第1の認証情報による暗号化を解除し、この受信したコピープロテクト対象のデータを、他のデバイスに送信する場合、送信先となる相手先デバイスとの間で認証処理を実施し、この認証処理によって生成、共有される第2の認証情報を取得し、前記送信元より受信した前記暗号化鍵を生成するためのパラメータ情報を、前記第2の認証情報により暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送するものである。

【0025】また、暗号化鍵により暗号化及び復号化可能なコピープロテクト対象のデータを扱うデータ処理装置において、データを受信する受信手段と、この受信手段

に受信された情報を他のデバイスに送信する送信手段と、前記他のデバイスとの間でコピープロテクト対象のデータを授受するための認証処理を行う認証手段とを具備し、送信元デバイスから前記コピープロテクト対象のデータを受信する場合、前記認証手段により前記送信元デバイスとの間で認証処理を実施し、この認証処理によって生成、共有される第1の認証情報を前記受信手段で取得し、前記送信元デバイスにより、前記第1の認証情報によって暗号化された前記暗号化鍵を生成するためのパラメータ情報を前記受信手段で受信すると共に、暗号化されたコピープロテクト対象のデータを受信し、前記認証手段により受信した前記パラメータ情報の前記第1の認証情報による暗号化を解除し、この受信したコピープロテクト対象のデータを、他のデバイスに送信する場合、前記認証手段で送信先となる相手先デバイスとの間で認証処理を実施し、この認証処理によって生成、共有される第2の認証情報を前記受信手段で取得し、前記送信手段により前記送信元より受信した前記暗号化鍵を生成するためのパラメータ情報を、前記第2の認証情報により暗号化して前記相手先デバイスに送信すると共に、前記コピープロテクト対象のデータを暗号化されたまま前記相手先デバイスに転送することを特徴とするデータ処理装置である。

【0026】また、本発明は、コンピュータシステムによって読み出し可能な記録媒体であって、コピープロテクト対象のデータが暗号化されて記録される第1の記憶領域と、前記暗号化データの暗号化を解除する暗号化解除情報を生成するために必要な情報を少なくとも第1及び第2の2つのパラメータに分けて記録する第2の領域を含み、前記第2の領域は、前記コンピュータシステムからは読み出せない領域であり、前記第1及び第2のパラメータは、コンピュータシステム内の複数のデバイスで共有可能な情報であることを特徴とする記録媒体である。

【0027】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。図1には、本発明の一実施形態に係るパーソナルコンピュータ（以下、PCと称する）のシステム構成が示されている。このPC11は、IEEE1394シリアルバス200を介して外部のコンシューマ電子機器、たとえば図示のようなセットトップボックス（STB）12、デジタルビデオカメラまたはDVカムコーダ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14と通信可能に構成されている。

【0028】セットトップボックス（STB）12、デジタルビデオカメラ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14は、それぞれIEEE1394コピープロテクト技術をサポートするために、IEEE1394シリアルバス200とのイン

ターフェイス部に、デバイス認証およびキー交換などを行う認証処理部 (Authenticator) 121, 131, 141を有している。コンテンツデータの送受信を行うセットトップボックス (STB) 12およびデジタルビデオカセットレコーダ (D-VCR) 14については、暗号化・復号化双方の機能を持つ暗号化/復号化部 (De-/Cipher) 122, 142が設けられている。また、コンテンツデータの送信のみを行うデジタルビデオカメラ (DVC) 13については、暗号化部 (Cipher) 132だけが設けられている。

【0029】PC11、セットトップボックス (STB) 12、デジタルビデオカメラ (DVC) 13、およびデジタルビデオカセットレコーダ (D-VCR) 14間で授受されるコンテンツデータは、暗号化された状態でIEEE1394シリアルバス200上を転送される。

【0030】PC11は、図示のように、PCIバス100と、これに接続された複数の機能モジュールとから構成されている。これら機能モジュールの中で、デジタルのコンテンツデータを扱う機能モジュール、つまり、CPUモジュール111、サテライトまたはデジタルTV用のチューナ113、MPEG2デコーダ115、DVD-RAMドライブ116については、PCIバス100とのインターフェイス部に、機器認証およびキー交換などを行う認証処理部 (Authenticator) 1111, 1131, 1151, 1161が設けられている。これら各認証処理部 (Authenticator) 1111, 1131, 1151, 1161の機能は、基本的に、1394デバイスであるセットトップボックス (STB) 12、デジタルビデオカメラ (DVC) 13、およびデジタルビデオカセットレコーダ (D-VCR) 14のそれと同じであり、コンテンツデータを暗号化して授受するために必要な認証およびキー交換を行う。

【0031】また、これらCPUモジュール111、チューナ113、MPEG2デコーダ115のインターフェイス部には、さらに、暗号化されたコンテンツ (encrypted contents) の暗号化を解除するための復号化処理を行う復号化部 (Decipher)、または暗号化部 (Cipher) が設けられている。暗号化部を持つか復号化部を持つか、あるいはその両方を持つかは各機能モジュールの機能によって決まる。ここでは、チューナ113については暗号化部 (Cipher) 1132が設けられ、CPUモジュール111およびMPEG2デコーダ115については復号化部 (Decipher) 1112, 1152が設けられている場合が例示されている。

【0032】CPUモジュール111は、マイクロプロセッサと、メモリコントローラ、およびPCIバスブリッジなどから構成されており、認証部1111と暗号解

除部1112は例えばPCIバスブリッジの一部として組み込むことができる。また、CPUモジュール111内の認証部1111、暗号解除部1112、MPEG2デコーダ部1113はソフトウェアで実現しても良い。

【0033】DVD-RAMドライブ116はPC11の補助記憶装置として設けられたものであり、IDEインターフェイスまたはATAPIインターフェイス等を介してPCIバス100に接続される。DVD-RAMドライブ116は認証処理部1161を有するが、復号化部 (Decipher)、暗号化部 (Cipher) については設けられていない。暗号化されたコンテンツデータを暗号化した状態のままDVD-RAM116に記録するためである。

【0034】PC11には、さらに、PCIバス100とIEEE1394シリアルバス200間を双方向で接続する1394ブリッジ117が設けられている。1394ブリッジ117には、認証処理部、暗号化部、復号化部はどれも設けられておらず、暗号化されたコンテンツデータは暗号化された状態のままPCIバス100からIEEE1394シリアルバス200へ、またIEEE1394シリアルバス200からPCIバス100に転送される。このように、1394ブリッジ117は、PC11内の機能モジュールと1394デバイスとの間を透過的に接続する。

【0035】ここで、IEEE1394シリアルバス200上のDVC13から転送されるデジタルコンテンツを、CPUモジュール111でソフトウェアデコードする場合の処理手順について説明する。

【0036】まず、DVC13とCPUモジュール111との間で機器認証を行い、互いにコピープロテクト機能を有する正当なデバイスであることを確認し合う。この機器認証は、たとえば、ランダムチャレンジ&レスポンス方法や、一方向関数を用いた方法、乱数を用いて毎回変わる時変数を使用する方法など、良く知られた方法を用いて実現できる。通信相手のデバイスがどのようなコンテンツの種類を扱うことができるものであるか否かの認証については、システムIDが用いられる。このシステムIDは、1394デバイスおよびPC11内の各機能モジュールの回路またはファームウェアなどに埋め込まれており、これによって、一回のみコピー可、コピー不可、コピーフリーの全種類のコンテンツデータを扱えるデバイスであるか、一回のみコピー可あるいはコピーフリーのコンテンツデータだけを扱えるデバイスであるかが判別される。

【0037】この認証処理にて、CPUモジュール111はDVC13より受け取ったデータに基づいて、暗号化されたコンテンツの暗号を解除するための暗号化鍵 (以下コンテンツキー) を生成する。DVC13は、コンテンツデータを暗号化し、それをCPUモジュール111に送る。暗号化されたコンテンツは暗号化されたま

ま1394バス200およびPCIバス100を介してCPUモジュール111に届き、CPUモジュール111の復号部(Decipher)1112は認証によって生成されたコンテンツキーを使ってコンテンツの暗号を解く。

【0038】暗号を解かれたコンテンツはCPUモジュール111内のソフトウェアMPEG2デコーダ(Decoder)1113によってデコードされた後、主メモリ112とVGAコントローラ114を直接結ぶAGP(Accelerated Graphics Port)10を介してVGAコントローラ114に送られて再生される。

【0039】このように、デジタルのコンテンツデータを扱う複数の機能モジュールそれぞれのインターフェイス部に認証処理部と、暗号化あるいは復号化部とを用い、機能モジュール間あるいは機能モジュールと1394デバイス間でコピープロテクト対象のデジタルコンテンツを受け渡すときに、それらデバイス間で認証処理およびコンテンツデータの暗号化・復号化処理を行う。IEEE1394バス200およびPCIバス100のどちらにおいても暗号化解除のためのキー、およびコンテンツデータは暗号化されたまま転送されるようになり、コンテンツデータの不正コピーを防止することができる。

【0040】また、PCI11内の各機能モジュール毎に認証処理を行うことができるので、機能モジュール単位で扱うことが可能なコンテンツデータの種類(一回のみコピー可、コピー不可、コピーフリー)を効率よく制限することが可能となる。

【0041】図2は本実施形態で用いられる認証処理およびキー交換の手順の一例が示されている。コンテンツを送信する側のデバイスがSource Device、受信する側のデバイスがSink Deviceである。

【0042】Sink Deviceは、まず、乱数を使って毎回変わる代わるランダムチャレンジキー(Na)を生成し、認証要求と共にそのランダムチャレンジキー(Na)を、Source Deviceに渡す。そして、Sink Deviceは、決められた関数を用いてNaからArを作成する。

【0043】Source Deviceは、乱数を使って毎回変わる代わるランダムチャレンジキー(Nb)を生成し、それを、認証要求に対する応答としてSink Deviceに返す。そして、Source Deviceは、決められた関数を用いてNbからBrを作成する。

【0044】この後、Source Deviceは、メッセージ(Bv)をSink Deviceに送る。このメッセージ(Bv)は、公開鍵と、Na、Brとから作成されたものである。

【0045】Sink Deviceは、メッセージ(Av)をSource Deviceに送る。メッセージ(Av)は、公開鍵と、Nb、Arとから作成されたものである。

【0046】Source Deviceは、Avが正しいか確認し、正しければ相手が正当なデバイスであると判断して認証鍵(Ak)を作る。同様に、Sink Deviceも、Bvが正しいか確認し、正しければ相手が正当なデバイスであると判断して認証鍵(Ak)を作る。

【0047】この後、Source Deviceは、認証鍵(Ak)で暗号化したコントロールキー(eKx)をSink Deviceに送る。Sink Deviceは、暗号化されたコントロールキー(eKx)を認証鍵(Ak)で暗号を解除し、コントロールキー(Kx)を作る。

【0048】なお、図2の認証処理の手順はあくまで一例であり、互いのデバイスが互いに正しいデバイスであることを検証し合うことができるものであれば、前述したように、通常のランダムチャレンジ&レスポンス方法や、その他の良く知られた方法を利用することができる。

【0049】図3は、本実施形態で用いられる認証処理およびコンテンツデータの暗号化処理、及びコンテンツデータの暗号化、復号化するための暗号化鍵(コンテンツキー(Kc))の作成手順に関する概念を示す図である。尚、図2と同様、コンテンツを送信する側のデバイスがSource Device、受信する側のデバイスがSink Deviceである。

【0050】以下図3の認証手順、暗号化手順について(1)から(10)まで各手順に従って説明していく。(1)まずSource DeviceとSink Deviceはお互いに認証処理を実施して互いに共有されるコントロールキー(Kx)を得る。尚、このコントロールキーは各機器間の認証処理により固有に共有される情報であり、他の機器間で認証処理をした場合には、また異なるコントロールキーが生成されることになる。この認証処理について詳細には図2で示したような方式をとる。

(2)Source Deviceは、コンテンツデータが、コピー不可、1回のみコピー可、コピーフリーのいずれであるかを示すCGMSと呼ばれるコピーコントロール情報(EMI)をSink Deviceに送信する。

(3)Source Device、Sink Deviceともに、コントロールキー(Kx)とコピーコントロール情報(EMI)を用いて、結合キー(Kck)を生成、Source Device、Sink Deviceで共有する。

【0051】この結合キーKckの生成処理を関数で表

すと、

$$Kck = J [Kx, EMI]$$

となる。

【0052】ここで、Source Deviceから送られるEMIがコピー一回可データを示している場合には、Sink Deviceでは、コピー不可を示す情報EMI' へ書き換えられ、以後自身がSource Deviceとして次の機器へコンテンツデータを送信する場合にはこのEMI' が送信されコンテンツデータのコピーが不可能になる。

(4) Source Deviceは、乱数発生器などによりランダムに発生されるシードキー(Kcs)を生成し、このシードキー(Kcs)を結合キー(Kck)を利用して暗号化を施し、暗号化されたシードキー(eKcs)をSink Deviceに送信する。

(5) Source Deviceは、さらに時刻等により内容が変わっていく時変数データ(Nc)を生成し、Sink Deviceに送信する。

(6) Source Deviceはコンテンツデータ(Contents)を暗号化、及び復号化するためのコンテンツキー(Kc)をシードキー(Kcs)と時変数データ(Nc)との関数に基づいて生成する。即ち関数で表すと、

$$Kc = J [Kcs, Nc]$$

となる。

(7) Source Deviceは生成されたコンテンツキー(Kc)を用いて、コンテンツデータ(Contents)を暗号化し、暗号化されたコンテンツデータ(e[Contents(Kc)])をSink Deviceに送信する。

(8) Sink Deviceは受信したコンテンツデータを復号化するためのSink Device自身でコンテンツキー(Kc)を生成する。このため、まず暗号化されたシードキー(e[Kck(Kcs)])を結合キー(Kck)により復号化し、シードキー(Kcs)を得る。

(9) そして、Sink Deviceはこのシードキー(Kcs)と、予め手順(5)により受け取った時変数(Nc)とのふたつのパラメータを元にしてコンテンツキー(Kc)をSink Device自身で生成。関数で示すと

$$Kc = J [Kcs, Nc]$$

として、Source deviceと同様の処理をしコンテンツキーを生成する。

(10) そして、Sink Deviceはコンテンツキー(Kc)を用いて、手順(7)で送られてきた暗号化されたコンテンツデータ(e[Contents(Kc)])を復号化して、正当にコンテンツデータ(Contents)を得ることができる。

【0053】以上このような認証手順、及び暗号化、復

号化手順を実施することにより、一つのコンテンツデータ(Contents)に対して、各機器間でコンテンツキー(Kc)を共有使用、つまり同一のコンテンツキー(Kc)を適正に転送することが可能になり、課題とされていた暗号化されたデータをさらに暗号化するような処理をする必要がなくなる。

【0054】転送可能になった理由は、機器間の認証により情報がその都度変わってしまうコントロールキー(Kx)や、CGMSのようにコンテンツデータのコピーにより、情報が書き換えられてしまうコピーコントロールキー(EMI)等可変のデータが、コンテンツキー(Kc)生成のための係数として直接使用しないで済むようにしたからである。このため本発明は、暗号化されたシードキー(Kcs)と、時変数(Nc)を利用してゐるものである。この際、シードキーの暗号化、及び復号化には機器間で変動する結合キー(Kck)を利用するが、シードキー(Kcs)及び時変数(Nc)を不変のデータとして扱えば、Sink Deviceが、Source Deviceとして次に別のデバイスにコンテンツデータに対して暗号化したコンテンツデータを転送する場合にも同じコンテンツキー(Kc)を生成、利用することができるので、コンテンツキー(Kc)で暗号化されたコンテンツデータ(e[Contents(Kc)])をさらにまた別のコンテンツキー(Kc')等で再度暗号化するような処理は必要なくなるのである。

【0055】次に、図2、図3を用いて説明した概念について各機器間での具体的な認証処理、暗号化処理についてそれぞれ説明していく。一般に、パーソナルコンピュータにおいて補助記憶装置として用いられるストレージデバイスには認証機能が設けられてないため、コピープロテクトが必要なコンテンツを記録することはできない。また、認証機能と復号化機能を用意すればコンテンツの暗号化を解除した後にストレージデバイスに記録することが可能となるが、このようにすると、今度は、その記録内容(Plain Contents)が不正に使用されてしまう危険がある。特に、可搬型の記録メディアを使用するリムーバブルストレージデバイスの場合には、その危険が高い。

【0056】そこで、本実施形態では、ストレージデバイスには認証処理部(Authenticator)のみを設け、コンテンツを暗号化したまま記録メディアに記録すると共に、さらに認証によって生成されたコンテンツキーを、システムがアクセスできない記録メディア上の領域に記録するようにしている。

【0057】以下、図4を参照しコピープロテクトが必要な一回のみコピー可のコンテンツデータをSTB12から受信してDVD-RAMドライブ116のDVD-RAMメディアに記録する場合を例示してその記録方法について具体的に説明する。

(1) STB12とDVD-RAMドライブ116それぞれの認証部(Authenticator)121、1161を使って、それらデバイス間の認証を行い、互いに正当なデバイスであることが確認されると、STB12側から暗号化されて送られて来るコントロールキー(eKx)をDVD-RAMドライブ116側で暗号を解きコントロールキー(Kx)を生成する。これにより同一のコントロールキー(Kx)をSTB12とDVD-RAMドライブ116で共有する。

(2) STB12が送信するコンテンツデータにはCGMSと呼ばれるコピーコントロール情報(EMI)が含まれており、このコピーコントロール情報(EMI)をDVD-RAMドライブ116にも送信して、図3により説明した関数に基づき結合キー(Kck)を共有する。

(3) STB12は、乱数発生器等によりランダムに発生されるシードキー(Kcs)を生成し、このシードキー(Kcs)を結合キー(Kck)を利用して暗号化されたシードキー(e[Kck(Kcs)])と、時変数データ(Nc)をDVD-RAMドライブ116に送信する。

(4) STB12は、シードキー(Kcs)と時変数データ(Nc)との関数に基づいてコンテンツキー(Kc)を生成し、このコンテンツキー(Kc)を利用して、コンテンツデータを暗号化する。そして、DVD-RAMドライブ116では暗号化されたコンテンツデータ(e[Contents(Kc)])を暗号化されたままPC1パス100を通してDVD-RAM116のメディア上に記録する。そして、対応する結合キー(Kck)によって一端シードキー(Kcs)を復号化し、これを時変数(Nc)と共に例えば、図5のようにセクター間のギャップ領域に記録される。この時シードキー(Kcs)と時変数(Nc)は、DVD-RAM116固有の情報である固有値(第3者機関により管理された秘密鍵等)によって暗号化を施され格納される。またコピーコントロール情報(EMI)は「一回コピー可」から「これ以上コピー不可」の状態(EMI')に書き換えられ、同様に暗号化されてギャップ領域に記録する。このギャップ領域はシステムからはアクセスできない領域である。尚、これら手順のコントロールは全てCPUモジュール111によって行われる。

【0058】次に、図6を参照して、DVD-RAMドライブ116のメディアに記録された暗号化されたコンテンツデータ(e[Contents(Kc)])をMPEG2デコーダ115で再生する場合について説明する。

(1) DVD-RAMドライブ116とMPEG2デコーダ115との認証部1161、1151間で、認証を行い互いに正当なデバイスであることが確認されると、DVD-RAM116側から暗号化されて送られて来る

コントロールキー(eKx)をMPEG2デコーダ115側で暗号を解きコントロールキー(Kx')を生成する。これにより同一のコントロールキー(Kx')をDVD-RAMドライブ116とMPEG2デコーダ115で共有する。

【0059】ただ、このコントロールキー(Kx')は上述したDVD-RAM115とSTB12とで生成したコントロールキー(Kx)とは異なっている。

(2) DVD-RAMドライブ116に格納されているコンテンツデータには「これ以上コピー不可」に書き換えられたコピーコントロール情報(EMI')が含まれており、このコピーコントロール情報(EMI')をMPEG2デコーダ115にも送信して、図3により説明した関数に基づき結合キー(Kck')を共有する。

【0060】(3) DVD-RAMドライブ116は、固有値で暗号化されて格納されていたシードキー(eKcs)に対して固有値を用いて復号化する。次にこの復号化されたシードキー(Kcs)を、今度は結合キー(Kck')を利用して暗号化し、この暗号化されたシードキー(e[Kck'(Kcs)])をMPEG2デコーダ115へ送信する。

【0061】これと同様に暗号化されて格納されていた時変数データ(eNc)についても固有値を用いて復号化し、MPEG2デコーダ115に送信する。

(4) DVD-RAMドライブ116は、コンテンツキー(Kc)より暗号化されたコンテンツデータ(e[Contents(Kc)])をMPEG2デコーダ116にそのまま送信する。

【0062】(ここで分かるように、シードキー(Kcs)、時変数(Nc)とコンテンツキー(Kc)は上述したSTB12とDVD-RAM116で利用したものと同じものを利用できる。従って、再度コントロールキーにより暗号化を施す必要はなく、既にコンテンツキー(Kc)を利用して暗号化されてDVD-RAM116に格納されたコンテンツデータ(e[Contents(Kc)])をMPEG2デコーダ116にそのまま送信することができる)

(5) MPEG2デコーダ116では、受信したコンテンツデータを復号化するために、MPEG2デコーダ116内のAuthenticator121で、暗号化されたシードキー(e[Kck'(Kcs)])を、結合キー(Kck')を用いて復号化し、シードキー(Kcs)を生成する。

【0063】(6) 次に、Authenticator121でシードキー(Kcs)と、DVD-RAMドライブ116より受け取っている時変数(Nc)との関数により、コンテンツキー(Kc)を生成する。

【0064】(7) 生成されたコンテンツキー(Kc)はMPEG2デコーダ115内のDe-Cipher1152に送られる。

(8) De-Cipher1152はKcにより暗号化されたコンテンツデータ(e[Contents(Kc)])をコンテンツキー(Kc)により解いて、そのコンテンツのPlainTextを生成する。

【0065】(9) MPEG2デコーダ115はPlainTextをデコードした後VGAコントローラ114のビデオ入力ポートに送り、それを画面表示する。以上のように、DVD-RAMドライブ116から、MPEG2デコーダ115にコピープロテクト処理の施されたコンテンツデータを送信する場合には、機器間の認証により生成される結合キー(Kck)や、コピーコントロール情報(EMI)は、STB12とDVD-RAMドライブ116でコピープロテクト処理をした場合とは異なっている。しかし、本実施形態のような方式をとることにより、コンテンツキー(Kc)については同一の情報を転送することができ、コピープロテクトを強固に保ったまま、MPEG2デコーダ115へDVD-RAMドライブ116に格納された暗号化されたコンテンツデータをそのままMPEG2デコーダに送信することができる。尚、これら手順のコントロールは全てCPUモジュール111によって行われる。

【0066】次に、図7を参照して、DVD-RAM上のメディアに記録された暗号化されたコンテンツデータ(EncryptedContents)を別のDVD-RAM上のメディアにコピーする場合について説明する。

【0067】この場合、Source DeviceとなるDVD-RAMドライブには、「コピー一回可」のコピーコントロール情報(EMI)が格納されていることを想定する。

(1) Source側DVD-RAMドライブ116とSink側DVD-RAM118に設けられている認証部1161、1181で、認証し互いに正当なデバイスであることが確認されると、Source側DVD-RAM116から暗号化されて送られて来るコントロールキー(eKx'')をSink側DVD-RAM117で暗号を解きコントロールキー(Kx'')を生成する。これにより同一のコントロールキー(Kx'')をDVD-RAMドライブ116とDVD-RAM118で共有する。

【0068】ただ、このコントロールキー(Kx'')は前記同様認証デバイス間で固有のコントロールキーを共有することになる。

(2) Source側DVD-RAMドライブ116に格納されているコンテンツデータには「コピー一回可」のコピーコントロール情報(EMI)が含まれており、このコピーコントロール情報(EMI)をSink側DVD-RAMドライブ117にも送信して、図3により説明した関数に基づき結合キー(Kck'')を共有する。

(3) Source側DVD-RAMドライブ116は、暗号化され格納されたシードキー(e'Kcs)に対して固有値を用いて復号化する。次にこの復号化されたシードキー(Kcs)を今度は結合キー(Kck'')を利用して暗号化し、この暗号化されたシードキー(e[Kck''(Kcs)])をSink側DVD-RAMドライブ117へ送信する。これと同様に暗号化されて格納されていた時変数データ(eNc)についても固有値を用いて復号化し、Sink側DVD-RAMドライブ118に送信する。

(4) Source側DVD-RAMドライブ116はKcにより暗号化されたままのコンテンツデータ(e[Contents(Kc)])をDVD-RAMドライブ118に送信し、DVD-RAMドライブ118では、このコンテンツデータ(e[Contents(Kc)])をそのままドライブ内のメディアに記録する。

(5) Sink側DVD-RAMドライブ118は、Source側DVD-RAMドライブ116から受け取った暗号化されたシードキー(e[Kck''(Kcs)])を、結合キー(Kck'')により復号化し、シードキー(Kcs)を生成する。

【0069】そして、このシードキー(Kcs)と時変数(Nc)とを、DVD-RAM118固有の情報(第3者機関により管理された秘密鍵等)によって暗号化を施され格納される。またコピーコントロール情報(EMI)は「一回コピー可」から「これ以上コピー不可」の状態に書き換えられ、同様に暗号化されてギャップ領域に記録する。このギャップ領域はシステムからはアクセスできない領域である。尚、これら手順のコントロールは全てCPUモジュール111によって行われる。

【0070】このように、DVD-RAMドライブから別のDVD-RAMドライブへコンテンツデータをコピーする場合には、コンテンツデータは初めから暗号化されたまま、復号化もされずそのままう一方のDVD-RAMドライブに転送されコピー処理が完了する。さらに、コンテンツキーを生成するためのシードキー(Kcs)、時変数(Nc)についても、そのまま同じデータが転送されることになる。

【0071】

【発明の効果】以上説明したように、本発明によれば、コンテンツデータを暗号化及び復号化するためのコンテンツキーを、各機器間での暗号化処理に共通に使用することができるので、暗号化されたコンテンツデータに対してさらに暗号化するような処理をすることなく、各機器間で同一の暗号化されたコンテンツデータを共有することができ、かつ強固なコピープロテクト機能を実現することが可能になる。

【図面の簡単な説明】

【図1】本発明の一実施形態に係るコンピュータシステムのシステム構成を示すブロック図。

【図2】図1のシステムにおける機器認証およびキー交換の一例を示す図。

【図3】同実施形態で使用される認証処理及びコンテンツデータの暗号化、復号化するための暗号化解除キー(Kc)の作成手順を示す概念図。

【図4】図1のシステムにおける、セットトップボックスからストレージデバイスへコンテンツデータ格納する動作を示す図。

【図5】同実施形態のシステムに設けられたストレージデバイスにおけるキーの記憶方式を説明するための図。

【図6】図1のシステムにおけるストレージデバイスから、再生手段へコンテンツデータを送信し、再生する動作を示す図。

【図7】図3で示されたコピープロテクト方式を用いて、ストレージデバイスから別のストレージデバイスへコンテンツデータを送信する動作を示す図。

【図8】コンテンツキー自体を受信装置側にそのまま送信しないで、受信装置側でコンテンツキーを作成する方式を説明するための図。

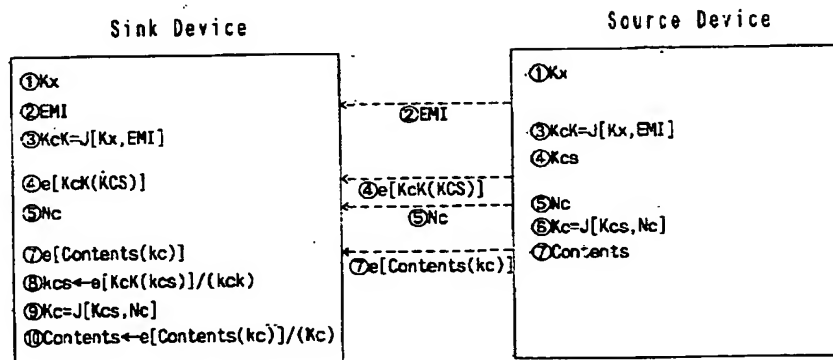
【符号の説明】

- 11…パーソナルコンピュータ(PC)
12…セットトップボックス(STB)
13…デジタルビデオカメラまたはDVカムコーダ(D*

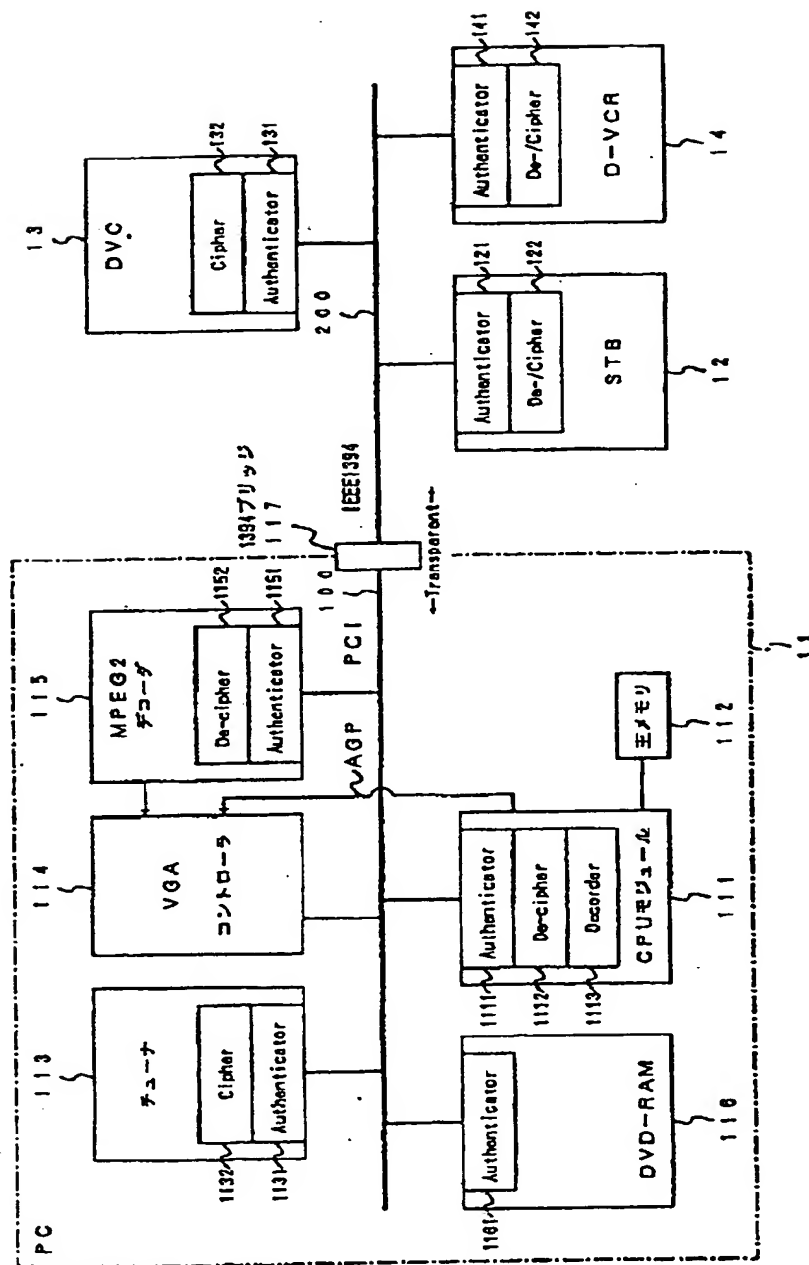
*VC)

- 14…デジタルビデオカセットレコーダ(D-VCR)
111…CPUモジュール
112…主メモリ
113…サテライトまたはデジタルTVチューナ
114…VGAコントローラ
115…MPEG2デコーダ
116…DVD-RAMドライブ
117…1394ブリッジ
121…認証部(Authenticator)
122…暗号化・復号化部(De-/Cipher)
131…認証部(Authenticator)
132…暗号化部(Cipher)
141…認証部(Authenticator)
142…暗号化・復号化部(De-/Cipher)
1111…認証部(Authenticator)
1112…復号化部(De-cipher)
1131…認証部(Authenticator)
1132…暗号化部(Cipher)
1151…認証部(Authenticator)
1152…復号化部(De-cipher)
1161…認証部(Authenticator)

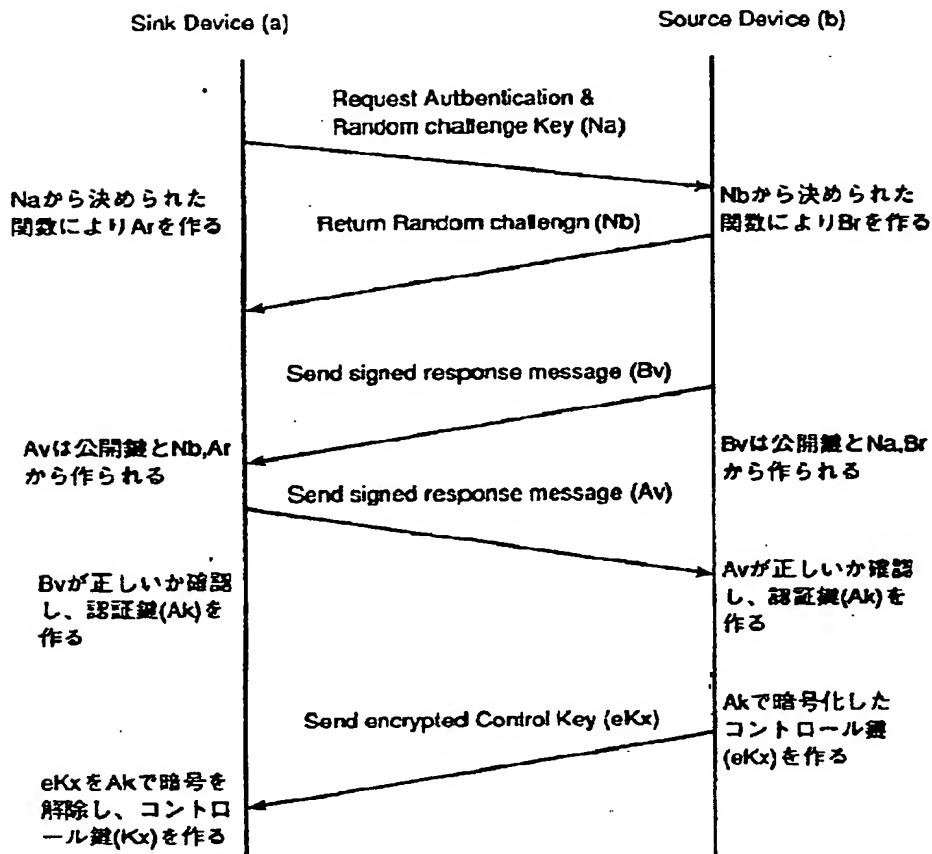
【図3】



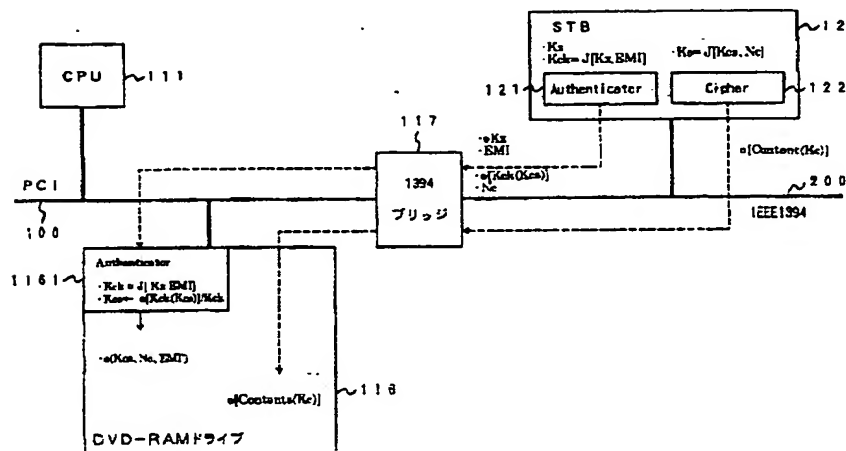
【図1】



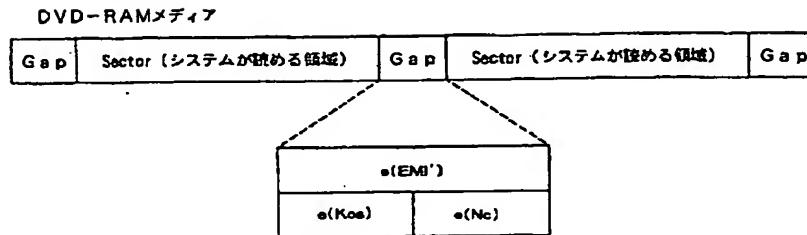
〔図2〕



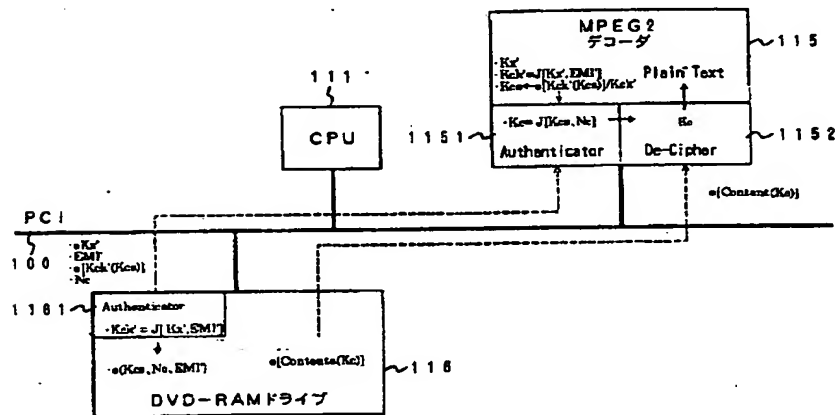
〔図4〕



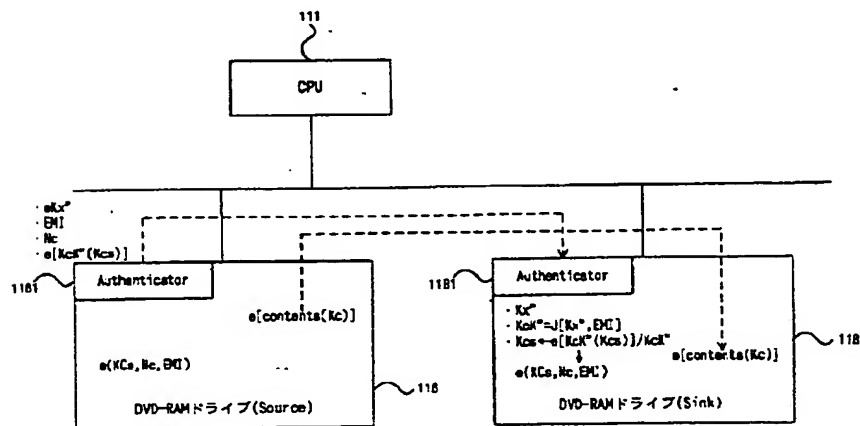
【図5】



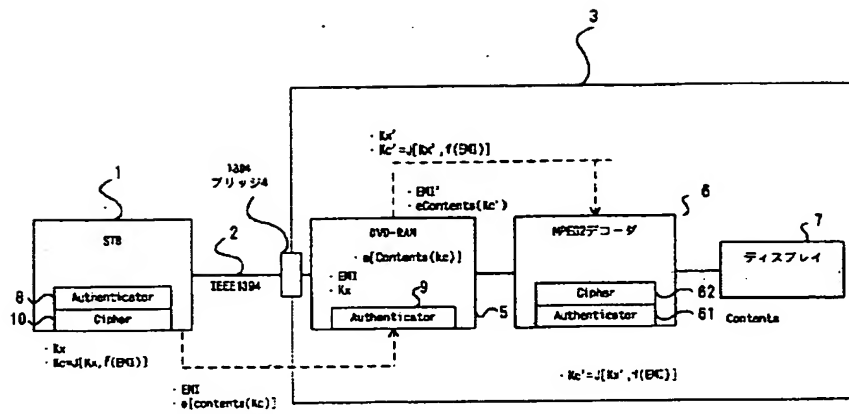
【図6】



【図7】



【図8】



フロントページの続き

(72)発明者 加藤 拓
東京都府中市東芝町1番地 株式会社東芝
府中工場内

F ターム(参考) SC064 BA01 BA07 BB05 BB07 BC06
BC07 BC17 BC22 CA14 CB01
CC04
5D044 AB05 AB07 BC06 CC04 DE49
GK08 GK17 HL08 HL11
5K013 EA02 FA03 GA04 JA00